CLAIMS

What is claimed is:

1. A computer software program for detecting whether or not there have been one or more specific changes in one or more application programs running on a computer system, comprising:

a storage medium;

an authentication program for authenticating a user prior to the execution of at least one of said application programs, and for associating the user in the aforementioned authentication to an application program that will be run later;

inspection scenarios, associated with each of said application programs and stored on said storage medium, for detecting whether or not there have been specific changes in each of said application programs; and

an inspection scenario program , stored on said storage medium, for detecting whether or not there has been a specific change in an application program, by running said associated specific application program according to said inspection scenario, and for outputting detection results in association with said user name and said application program.

2. A computer software program article as set forth in Claim 1, wherein:

said one or more application programs includes an application program executor for displaying the other application programs to the user selectively and executably.

3. A computer software program as set forth in Claim 1, wherein:

said one or more application programs is a plurality of application programs requiring validations in order to fulfill specific standards under identical policies;

said inspection scenarios are for detecting whether or not changes in each application program are to the degree that allows execution of the application program without performing a re-validation; and

said inspection scenario program instructs said computer system to display the detection result, when, in accordance with said inspection scenario, a change of an extent greater than that wherein execution is allowed without performing validations is detected.

4. A computer software program as set forth in Claim 1, wherein:

said inspection scenario program inputs a dummy signal into said application program in accordance with said inspection scenario to detect a response signal to said inputted dummy signal, to thereby detect whether or not there has been a specific change in the application program.

5. A computer software program as set forth in Claim 4, wherein:

said inspection scenario includes at least data for specifying an application program to be subjected to inspection, data for inputting as dummy signals into said application program, and data regarding an allowable range regarding the response to said data.

6. A computer software program as set forth in Claim 1, wherein:

said inspection scenario program is run at specific time intervals.

7. A computer software program as set forth in Claim 1, wherein:

said inspection scenario program comprises a detection results display unit for displaying said detection results on a computer display, and a user input/output unit for receiving user input regarding said detection results and for outputting in association with said detection results.

8. A computer software program as set forth in Claim 1, wherein said authentication program:

comprises an authentication update requesting unit for requesting the input of user authentication data at each specific time interval; and

if the user cannot be authenticated by said authentication update requesting unit, terminates said application program that is running, associated with the applicable user.

9. A computer software program as set forth in Claim 1, wherein:

said authentication program performs repeat user authentication in response to a user request after an initial user authentication, and associates, with the user involved in said authentication, the application programs currently running, and application programs run thereafter.

10. A computer software program as set forth in Claim 1, wherein said computer software program is for insuring that the results of safety testing have not been falsified or tampered with in said application program; and

wherein said application program receives measurement values, which have not been falsified or tampered with, from a measurement device for safety testing, processes the measurement values, and outputs the results of specific processing.

11. An application program inspecting system comprising:

an application storage unit for storing one or more mutually-related application programs;

an authentication unit for performing user authentication prior to running at least the first of said application programs, and for associating application programs run thereafter, with the user involved in said authentication;

an inspection scenario storage unit for storing inspection scenarios, associated with each of said application programs, for detecting whether or not there have been specific changes in each of said application programs; and

an inspecting unit for detecting whether or not there have been specific changes in said application programs, through an inspection scenario program executing specific related application programs in accordance with said inspection scenarios, and for outputting said detection results in association with said user name and application program.

12. A method for detecting whether or not there have been one or more specific changes in one or more mutually-related application programs on a computer system, comprising:

an authentication process for performing user authentication prior to running at least the first of said application programs and for associating, with said application programs run thereafter, the user involved in said authentication;

and an inspection process for detecting whether or not there has been a specific change in said application program, through the use of an inspection scenario, associated with each application program, for detecting whether or not there has been a specific change in each of the application programs, by an inspection scenario program executing a specific related application program in accordance with said inspection scenario, and outputting the detection results in association with said user name and application program.